(12) UK Patent Application (19) GB (11) 2 324 935 (13) A

(43) Date of A Publication 04.11.1998

(21) Application No 9708911.4

(22) Date of Filing 01.05.1997

(71) Applicant(s)
Motorola Limited
(Incorporated in the United Kingdom)
Jays Close, Viables Industrial Estate, BASINGSTOKE, Hampshire, RG22 4PD, United Kingdom

(72) Inventor(s)
William Neil Robinson

(74) Agent and/or Address for Service
Sarah J Spaulding
Motorola Limited, European Intellectual Property Operation, Midpoint, Alencon Link, BASINGSTOKE, Hampshire, RG21 7PL, United Kingdom

(51) INT CL^6
H04L 9/32 , G06F 1/00 12/14 , H04L 12/22

(52) UK CL (Edition P)
H4P PDCSA
G4A AAP

(56) Documents Cited
GB 2241133 A EP 0456386 A2 US 5400403 A
US 5349643 A

(58) Field of Search
UK CL (Edition O) G4A AAP , H4L LECC , H4P PDCSA PPEB
INT CL^6 G06F 1/00 12/14 , H04L 9/32 12/22
Online : WPI

(54) Abstract Title
Prevention of unauthorised data download

(57) A system for the prevention of unauthorised data download comprises a client computer (101) capable of downloading data from a source computer (not shown), the client computer (101) having a store (212) for receiving a validation code other than from the source computer and being provided with an authorisation module (200) arranged to use the validating code so as to verify whether the client computer (101) is authorised to download the data from the source computer. The source computer enables the authorisation module (200) by transmitting or activating validating means, such as a Software Authorisation Agent where the data is software.

The data can be text, images, music or other audio, and the infrastructure can be a cellular telephone (GSM), or UMTS, or infra red system.

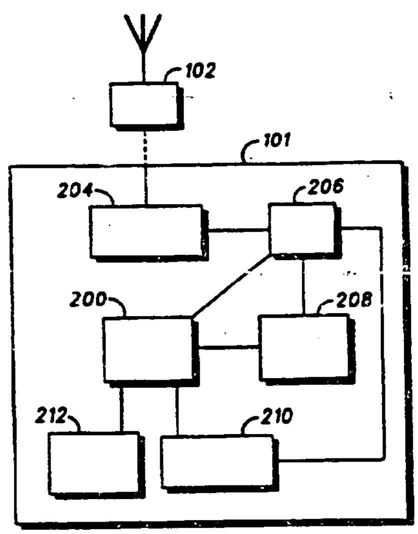

FIG.2

GB 2 324 935 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

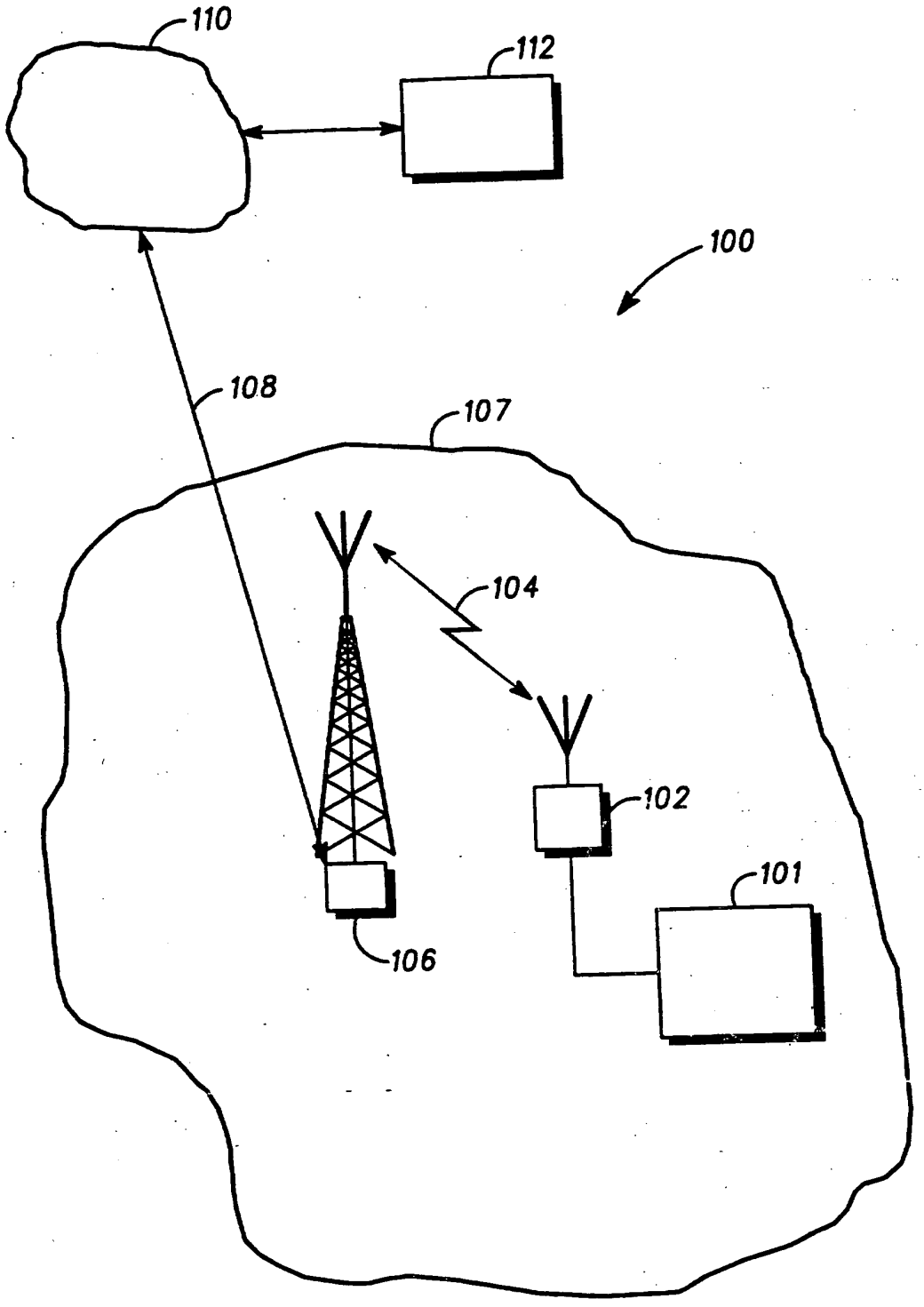

FIG.1

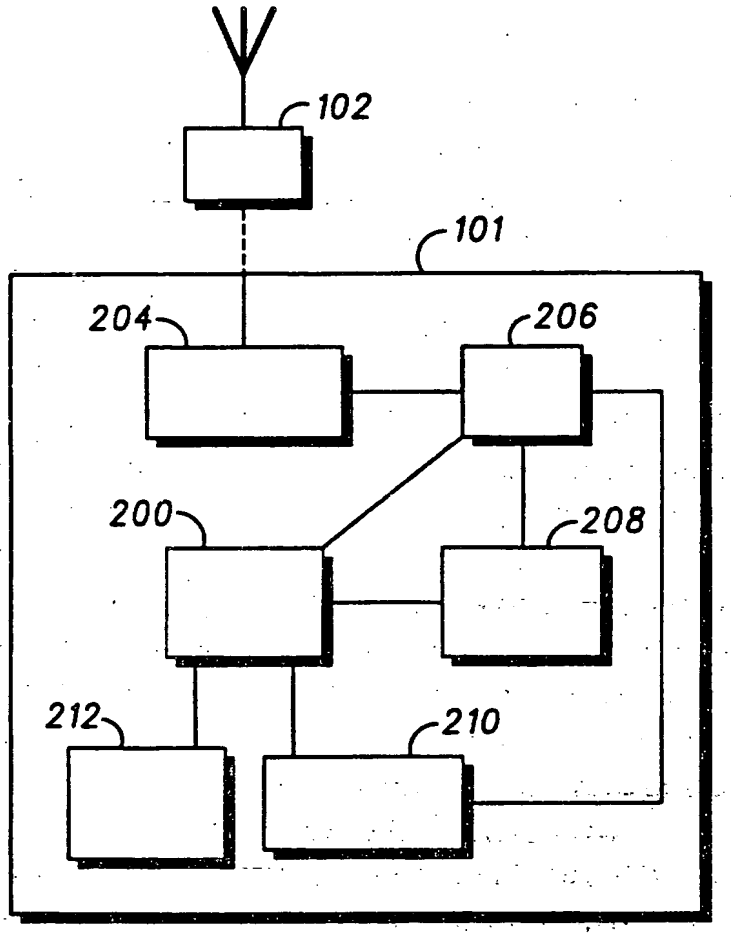

FIG. 2

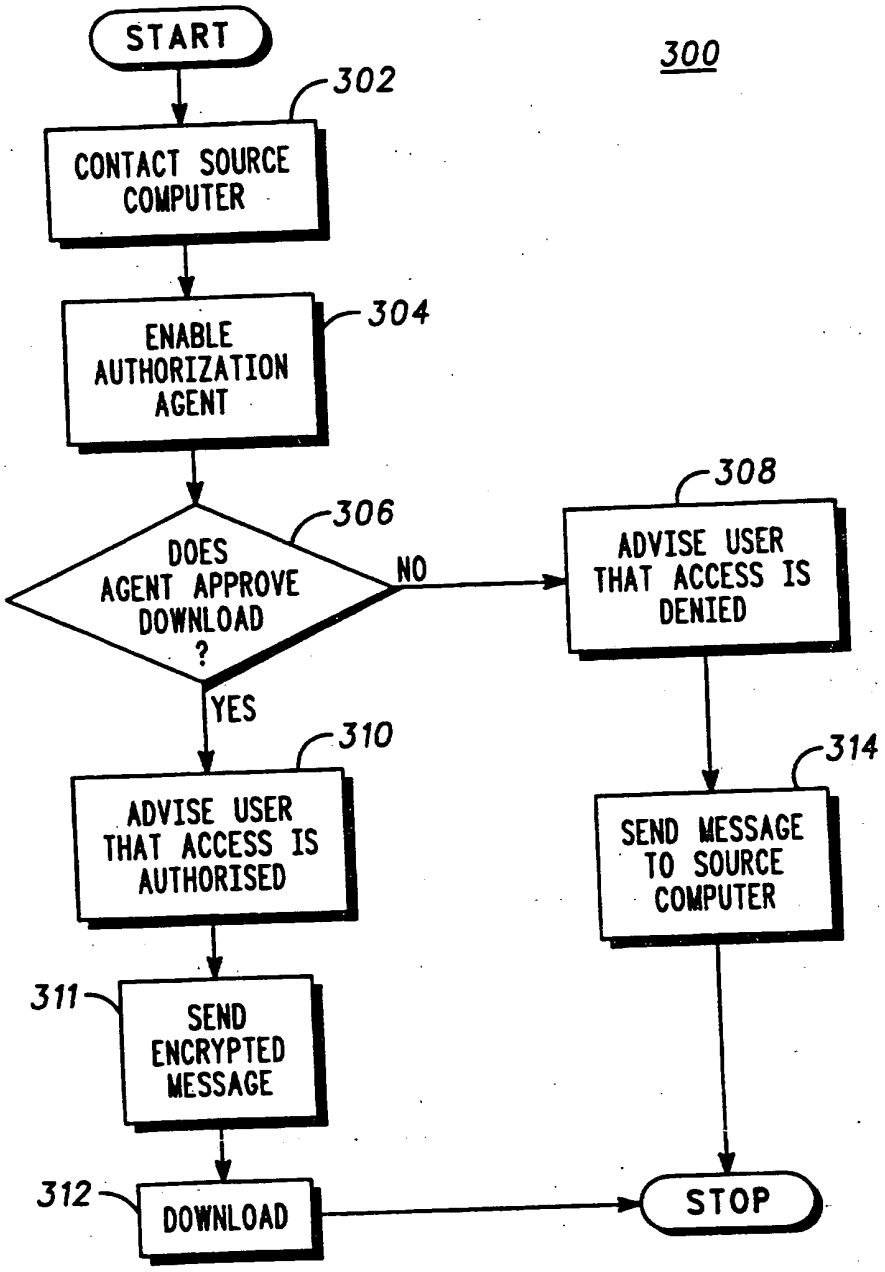

FIG. 3

SYSTEM, METHOD AND APPARATUS FOR THE PREVENTION OF UNAUTHORISED DATA DOWNLOAD

Field of the Invention

The present invention relates to a system, method and apparatus for the prevention of unauthorised data download, in particular, the prevention of unauthorised software download.

Background of the Invention

It is known to download computer software from a source computer to a client computer via an infrastructure, for example, an Internet site, to a terminal. Such a system is described in US 4, 528, 643, which relates to any digital system where purchased software is downloaded to disk, or is already stored on disk, but can only be accessed with a decryption code received after electronic payment. However, bandwidth of the infrastructure is wasted if a user discovers subsequently that execution of the software is not authorised, thereby also reducing the capacity and so the effectiveness of the infrastructure. Also, the user is charged for any "air time" used to download the software, even though the software cannot be executed. Thus, once downloaded, the software is not executable by the user and so resources have been wasted. An additional inconvenience is also suffered by the user, since an un-user friendly delay will exist between initiation of the download of the software and the user becoming aware that execution of the software is not possible, especially if the software is large. These disadvantages are particularly pertinent when the software is downloaded via a radio frequency infrastructure.

DE-A1-4 404 327 discloses a system comprising a source computer and a client computer, both possessing a code. The code possessed by the source computer is transmitted to the client computer for comparison before data is downloaded from the source computer to the client computer.

A more sophisticated version of the above described code, known as a Software Validation Certificate, can be used and can contain information relating to system privileges possessed by the software, for example, full access to all device hardware and software function, and ability to execute only with no access to other programs, data or hardware. The certificate, or the above-described codes, are downloaded with the software; the code (as described in relation to US 4, 528, 643 and DE-A1-4 404 327) or the certificate is transmitted to the client computer and so is susceptible to fraud, for example, an individual possessing equipment to receive the code can achieve execution of the software without payment.

It is therefore an object of the present invention to obviate or mitigate the above mentioned disadvantages relating to the downloading of data.

Summary of the Invention

According to a first aspect of the present invention, there is provided a system for the prevention of unauthorised data download comprising a first communicating means capable of downloading data from a second communicating means, the first communicating means having a store for receiving a validation code and being provided with a validating means arranged to use the validating code so as to verify whether the first communicating means is authorised to download the data from the second communicating means.

According to a second aspect of the present invention, there is provided a method of preventing unauthorised download of data in a system having a first communications means capable of downloading data from a second communications means, the method comprising the steps of:

obtaining a validation code,

requesting download of data from the second communications means,

verifying that the first communications means is authorised to download the data using the validation code.

According to a third aspect of the present invention, there is provided a data terminal apparatus comprising a communicating means for receiving data from a second communicating means, a store for receiving a validation code other than from the second communicating means, and a validating means arranged to use the validating code to verify whether the first communications means is authorised to download data from the second communications means.

Other, preferred, features and advantages are set forth in dependent Claims 2 to 20, 23 to 29 and the following description and drawings.

It is thus possible to provide a system which, in terms of resources, increases the efficiency of the infrastructure (especially in the case of a radio frequency infrastructure), whilst preventing unauthorised reception, either directly or indirectly (by a third party), of the data downloaded. Also, it is possible to provide a reduced turn-around time between requesting download and denial of download; the turn-around time between requesting authorisation and authorisation should remain substantially unchanged.

Brief description of the Drawings

The invention will now be described in more detail, with reference to the accompanying drawings, in which:

FIG. 1 shows a system which is capable of constituting an embodiment of the present invention,

FIG. 2 is a schematic diagram of a computer constituting an embodiment of the present invention, and

FIG. 3 is a flow diagram of a method for use with the system and computer of FIG. 1 and FIG. 2.

Description of a Preferred Embodiment

Referring to FIG. 1, a system 100 comprises a client computer 101 located within a geographical area 107 and capable of communicating with a source computer 112. Although the client computer 101 is used in this example, other devices can be used, for example, any remote destination device. The client computer 101 is connected to a cellular telephone 102, which is in communication with a Base Transceiver Station (BTS) 106, via a radio interface 104. It is conceivable to combine the cellular telephone 102 with the client computer 101 in a single unit. The BTS is connected to a wire line infrastructure 110, for example, an Integrated Service Digital Network (ISDN), via a cellular infrastructure 108, for example, a Global System for Mobile communication (GSM), the wire line infrastructure 110 being connected to the source computer 112 from which download of software is desired.

Although the source computer 112 has been described as being connected to the client computer 101 via a cellular infrastructure 108, other infrastructures are envisaged, for example, any wireless system, such as a Universal Mobile Telephone System (UMTS) or an infra-red system. Alternatively, the cellular telephone 102 and the cellular infrastructure 108 can be replaced with a modem (not shown) connected directly to the wire line infrastructure 110.

The client computer 101 possesses an I/O card 204 (FIG. 2) for interfacing the client computer 101 with the cellular telephone 102. The I/O card 204 is connected to a processing unit 206, the structure and function of which is known in the art. The structure of the processing unit 206 is not considered relevant to the present invention and so will not be described in any further detail. The processing unit 206 is connected to an authorisation module 200 and a download store 208 for storing downloaded data, including software.

The authorisation module 200 is also connected to the I/O card 204 via the processing unit 206. The download store 208, a certificate store 212 and a Man Machine Interface (MMI) 210, for example, a keyboard and a display, a

touch-screen or a voice recognition unit, the MMI 210 also being connected to the processing unit 206.

During normal operation (FIG. 3), a user is pre-provided with a Software Validation Certificate (SVC) from the proprietor of the source computer 112 and which is stored in the certificate store 212. Optionally, a Device Authorisation Certificate (DAC) can also be loaded into the certificate store 212 and used to determine whether the client computer 101 is licensed, or allowed, to execute the downloaded software. When the user wishes to download software from the source computer 112, for example pre-paid software, the user instructs the client computer 101 to contact the source computer 112 using the cellular telephone 102 (step 302).

Once the source computer 112 has been contacted, the source computer enables the authorisation module 200 (step 304). This is achieved by either transmitting a Software Authorisation Agent (SAA) to the client computer for storage in the authorisation module 200, or by having the SAA pre-resident in the authorisation module 200 and activating the SAA via a message from the source computer 112. Information relating to the SVC or DAC is included within the SAA. Although, in this example, the SAA, is a computer program, or a suite of computer programs/processes, the SAA can be embodied by other techniques known in the art to validate the SVC, for example, an electronic circuit.

Once the SAA is enabled, or if appropriate, downloaded and enabled, the SAA verifies whether the SVC is valid, and so download of the software is authorised or invalid and download should be denied (step 306). If the SVC is valid, the user is advised, via the MMI 210, that download of the software is authorised (step 310) and an encrypted message is sent to the source computer 112 (step 311), after which download of the software from the source computer 112 to the client computer 101 takes place (step 312), the downloaded software being stored in the download store 208. Optionally, the downloaded software can be encrypted and the SAA can be provided with a decryption key for decrypting the encrypted software. The decryption key can be a function of the SVC or the DAC. If desirable, the SAA can perform

the decryption of the downloaded encrypted software. Additionally, the source computer 112 can interrogate the client computer 101 in order to ascertain what preferences , if any, relating to the software the user might have, for example, language, configuration, or version. The user is then free to execute the software. If, however, the SVC is not valid, the user is advised, via the MMI 210, that download of the software is denied (step 308) and the source computer 112 is sent a download denied message to this effect (step 314). The download denied message can be encrypted. Optionally, the user can be advised, via the MMI 210, as to the reason for the download being denied and any possible recommended subsequent action which can be take by the user, for example, contacting the software licensor for authorisation.

Once the user has been advised that download is denied or download has been authorised and the software downloaded, the SAA can subsequently be deleted from the authorisation module 200.

The SAA can also be empowered to validate the DAC. The DAC can optionally be downloaded from the source computer 112 to the client computer 101 with the SAA. Other authorisation tests known in the art can also be carried out by the SAA, for example, the SAA can determine whether the client computer 101 is capable of handling a software watermark which can be present in the software to be downloaded.

Although the above example has been described in the context of downloading software, it is not intended that the present invention be limited to software alone, and should include the downloading of any data, for example, text, images or music and other audio information.

Additionally, even though the source computer has been charged with the task of sending the SAA and communicating with the SAA in the above example, it is not intended that the invention be limited to this example. It is envisaged that the infrastructure being used can also handle the transmission of and communication with the SAA.

It is also conceivable to implement the above invention in the context of other digital telecommunications systems than those mentioned above, for example, a Future Public/Private Land Mobile Telecommunications System (FPLMTS), a Personal Communications System (PCS), Cable Television system, or an Intelligent Transportation System (ITS).

The above embodiments can be implemented via the exchange of information between the SAA and a software environment which is resident in the client computer 101. The interface between the SAA and the software environment can be an Application Programmers Interface (API). The existence of APIs is known in the art.

Claims

1. A system for the prevention of unauthorised data download comprising a first communicating means capable of downloading data from a second communicating means, the first communicating means having a store for receiving a validation code and being provided with a validating means arranged to use the validating code so as to verify whether the first communicating means is authorised to download the data from the second communicating means.

2. A system as claimed in Claim 1, wherein the validating means is pre-resident in the first communicating means.

3. A system as claimed in any one of the preceding claims, wherein the first communicating means is provided with the validating means by downloading the validating means to the first communicating means from the second communicating means.

4. A system as claimed in any one of the preceding claims, wherein the validating means is erasable.

5. A system as claimed in any one of the preceding claims, further comprising encryption means arranged to send an encrypted message from the first communicating means to the second communicating means.

6. A system as claimed in any one of the preceding claims, wherein the encrypted message is a function of the validation code.

7. A system as claimed in any one of the preceding claims, wherein the data is encrypted and the validating means is arranged to provide the first communicating means with a decryption key.

8. A system as claimed in Claim 7, wherein the data is decrypted by the validating means.

9. A system as claimed in any one of the preceding claims, wherein the encryption of the data is a function of the validating code.

10. A system as claimed in any one of the preceding claims, wherein the validating means is resident in the first communicating means and communicates with a software environment via an application programmers interface.

11. A system as claimed in any one of the preceding claims, wherein the validating code is a software validation certificate.

12. A system as claimed in any one of the preceding claims, wherein the validating code is a device authorisation certificate.

13. A system as claimed in any one of the preceding claims, wherein the validating means is a software authorisation agent.

14. A system as claimed in any one of the preceding claims, wherein the store is arranged to receive the validation code other than from the second communicating means.

15. A system as claimed in any one of the preceding claims, wherein the data includes computer software.

16. A system as claimed in any one of the preceding claims, wherein the data includes text.

17. A system as claimed in any one of the preceding claims, wherein the data includes image data.

18. A system as claimed in anyone of the preceding claims, wherein the data includes audio data.

19. A radio frequency communications system comprising the system as claimed in any one of the preceding claims.

20. A wire line communications system comprising the system as claimed in any one of Claims 1 to 18.

21. A system for the prevention of unauthorised data download substantially as hereinbefore described with reference to FIG. 1 and FIG. 2.

22. A method of preventing unauthorised download of data in a system having a first communications means capable of downloading data from a second communications means, the method comprising the steps of:

obtaining a validation code,

requesting download of data from the second communications means,

verifying that the first communications means is authorised to download the data using the validation code.

23. A method as claimed in Claim 22, further comprising downloading a validating means from the second communications means.

24. A method as claimed in Claim 22, further comprising providing a validating means pre-resident in the first communications means.

25. A method as claimed in any one of Claims 22 to 24, further comprising erasing the validating means one the verification as to whether the first communications means is authorised to download the data from the second communications means has taken place.

26. A method as claimed in any one of Claims 22 to 25, further comprising sending an encrypted message from the first communications means to the second communications means.

27. A method as claimed in any one of Claims 22 to 26, further comprising encrypting the data prior to downloading the data to the first communications means and providing the first communications means with a decryption key.

28. A method as claimed in any one of Claims 22 to 27, wherein the validation code is obtained other than from the second communications means.

29. A method as claimed in any one of Claims 23 to 28, wherein the validating means is resident in the first communicating means and communicates with a software environment via an application programmers interface.

30. A method of preventing unauthorised download of data in a system substantially as hereinbefore described with reference to FIG. 3.

31. A data terminal apparatus comprising a communicating means for receiving data from a second communicating means, a store for receiving a validation code other than from the second communicating means, and a validating means arranged to use the validating code to verify whether the first communications means is authorised to download data from the second communications means.

The Patent Office

12

Application No: GB 9708911.4
Claims searched: 1-31

Examiner: Keith Williams
Date of search: 18 July 1997

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): G4A (AAP); H4L (LECC); H4P (PDCSA, PPEB)

Int Cl (Ed.6): G06F 1/00, 12/14; H04L 9/32, 12/22

Other: Online WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2241133 A	Motorola Inc. - see page 2, line 1 onwards.	1,22,31
X	EP 0456386 A2	ICL - see pages 4 and 5	1,22,31
A	US 5400403	RSA Data Security - see abstract	1,22,31
X	US 5349643	IBM Corp. - see column 2, line 63, to column 3, line 27	1,22,31

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.